Monthly newsletter GDPR: Accountability Privacy by Design and Privacy by Default

April 18, 2017

Introduction

This fourth edition of the GDPR newsletter, the first after our tie-up with Dentons, deals with the (new) data protection principles of accountability, privacy by design and privacy by default.

Under the Dutch Personal Data Protection Act (the DPA) organisations processing personal data are required to notify the supervisory authority (the Autoriteit Persoonsgegevens) about their processing. Under the GDPR organisations will be no longer obliged to report their processing. Instead, more responsibilities arise for organisations in this respect. The GDPR places emphasis on the principle of 'accountability', which requires organisations to take all technical and organisational measures to comply with the principles and obligations arising from the GDPR. It furthermore requires organisations to be able to demonstrate this compliance. As expected, the newly introduced data protection principles will have a major impact on organisations' current practices.

Under the GDPR, organisations shall have to (i) keep detailed records of their personal data processing activities, (ii) where applicable, undertake a privacy impact assessment and (iii) implement data protection by design and by default.

The accountability principle

Article 5 (2) GDPR introduces the accountability principle:

"The controller shall be responsible for, and be able to demonstrate compliance with paragraph 1 ('accountability')."

"Paragraph 1" refers to Article 5 (1) GDPR that lists the principles relating to personal data processing. In accordance with Article 5 (1) GDPR personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject;
- collected for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; and

- processed in a manner that ensures appropriate security of the personal data.

Organisations processing personal data shall be responsible for and must be able to demonstrate compliance with all of the aforementioned principles. Additionally, organisations must be able to substantiate their decisions made regarding the aforementioned and, again, be able to demonstrate their substantiation.

Article 24 GDPR sets out an example of the codification of the principle of accountability. Controllers are required to:

“implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.”

The way in which the data controllers must exactly demonstrate data processing in accordance with the GDPR is not specifically formulated. Further guidance from the Article 29 Working Party (WP 29) on this may be expected prior to 25 May 2018 (the date as of which the GDPR shall apply).

Records of processing activities

A more concrete implementation of the concept of accountability can be found in Article 30 GDPR, which obliges most data controllers and data processors to maintain a written (including electronic) record of processing activities under their responsibility[1]. The written or electronic record shall at least contain:

1. the name and contact details of the controller and, where applicable, the joint controller, the controller’s representative and the data protection officer;
2. the purposes of the processing;
3. a description of the categories of data subjects and categories of personal data;
4. the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
5. where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, where applicable, the documentation of suitable safeguards;
6. where possible, the envisaged time limits for erasure of the different categories of data; and
7. where possible, a general description of the technical and organisational security measures.

Also processors must maintain a record of all categories of processing activities on behalf of their data controllers. The electronic or written record shall at least contain:

1. the name and contact details of the processor and of each controller on behalf of which the processor is acting and, where applicable, of the controller’s or the processor’s representative, and the data protection officer;
2. the categories of processing carried out on behalf of each controller;
3. where applicable, transfers of personal data to a third country or an international organisation and, where applicable, the documentation of suitable safeguards; and
4. where possible, a general description of the technical and organisational security measures.

The principles of privacy by design and privacy by default

The principles of privacy by design and privacy by default oblige organisations to consider data privacy at the initial

design stages of products and services as well as throughout the whole process.

Privacy by design

Privacy by design is primarily of importance when developing new products and services. According to Article 25 (1) GDPR the controller is, both at the time of determining the means for processing and at the time of processing itself, obliged to implement appropriate technical and organisational measures, which are designed to implement data-protection principles, in an effective manner and to integrate the necessary safeguards into the processing.

Organisations have to make sure and be able to prove that data protection is a main focus from the early stages of the design process. Adapting the relevant systems to comply with the GDPR in a more advanced stage may lead to unnecessary costs.

Privacy by default

Article 25 (2) GDPR requires data controllers to implement appropriate technical and organisational measures for ensuring that, by default, only personal data which is necessary for each specific purpose of the processing is processed. This obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of people.

The principle of privacy by default is primarily of importance for services and products where the data subject has the choice of sharing its personal data. Privacy by default obliges organisations to protect the privacy of data subject by applying the most privacy friendly settings. In particular, this principle plays an important role in personal data processing related to online and social media platforms. In principle, pre-ticked boxes and applications automatically tracking data subject's location do not meet the requirements of privacy by default.

How to comply?

Organisations must adopt internal policies and implement measures which meet the principles of data protection by design and data protection by default. Such measures include minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subjects to monitor the data processing, and enabling the data controller to create and improve security features.

When developing, designing, selecting and using applications, services and products which are based on the processing of personal data or the use of which entails processing personal data, producers should be encouraged to take into account the right to data protection to make sure that controllers and processors are able to fulfil their data protection obligations.

An approved certification mechanism may be used as an element to demonstrate compliance with the requirements of privacy by design and privacy by default.

Practical recommendations and conclusion

From the moment the GDPR applies, it will no longer be the supervisory authority that keeps records of personal data processing within organisations. Instead, it will be the controller, subject to accountability, which shall keep updated records of its processing. Taking also into account the principles of privacy by design and privacy by default, logically adaptions in internal policies and technical systems are required within a majority of organisations.

It will take considerable time to map all personal data processing activities, especially for larger organisations

processing a significant amount and several types of personal data. All changes should be implemented by 25 May 2018. From that date, the supervisory authorities shall actively monitor and enforce the application of the GDPR. The supervisory authorities will be authorised to impose serious administrative fines on organisations not acting in compliance with the GDPR. We therefore recommend to start implementing the GDPR in time. Mapping the various personal data processing activities within your organisation is a good way to start this process.

Please click here to subscribe to our monthly updates on the GDPR.

Overview of subjects

January 2017	Territorial scope of the GDPR (Dutch)
February 2017	The Concept of Consent
March 2017	Sensitive Data
April 2017	Accountability, Privacy by Design and Privacy by Default
May 2017	Rights of Data Subjects (information notices)
June 2017	Rights of Data Subjects (access, rectification and portability)
July2017	Rights of Data Subjects (erasure, restriction, object and automated individual decision-making)
August 2017	Data Processors
September 2017	Data Breaches and Notifications
October 2017	Data Protection Officers
November 2017	Transfer of Personal Data (outside the EEA)
December 2017	Regulators (competence, tasks and powers)
January 2018	One Stop Shop
February 2018	Sanctions
March 2018	Processing of Personal Data in Employment Context
April 2018	Profiling and Retail
May 2018	Overview

1. The obligation to maintain a register of data processing activities does not apply to an organisation that employs fewer than 250 employees, unless the processing (i) is likely to result in a risk to the rights and freedoms of data subjects; (ii) is not occasional; or (iii) includes special categories of data (see our previous newsletter). The exception is therefore narrow and most organisations shall be obliged to maintain the register. ↩

Your Key Contacts

Marc Elshof
Partner, Amsterdam
D +31 20 795 36 09
M +31 6 46 37 61 08
marc.elshof@dentons.com

Celine van Es
Associate, Amsterdam
D +31 20 795 31 22
M +31 6 11 16 30 45
celine.vanes@dentons.com